KONINKRIJK DER NEDERLANDEN

Bureau voor de Industriële Eigendom

Hierbij wordt verklaard, dat in Nederland op 16 oktober 2003 onder nummer 1024547,

ten name van:

KONINKLIJKE KPN N.V.

te Groningen

een aanvrage om octrooi werd ingediend voor:

"Werkwijze voor het gebruik van elektromagnetische kraskaart voor het leveren van diensten",

onder inroeping van een recht van voorrang, gebaseerd op de in Nederland op

31 maart 2003 onder nummer 1023058 ingediende aanvrage om octrooi, en

dat de hieraan gehechte stukken overeenstemmen met de oorspronkelijk ingediende stukken.

Rijswijk, 27 januari 2004

De Directeur van het Bureau voor de Industriële Eigendom,
voor deze,

Mw. M.M. Enhus

CERTIFIED COPY OF
PRIORITY DOCUMENT

1024547

UITREKSEL

De uitvinding betreft een systeem en een werkwijze voor het middels een elektromagnetische kraskaart (1) leveren van diensten tussen een voor een dienstafnemer toegankelijke terminal (6) en een infrastructuur. Het systeem omvat een netwerk (7) en een server (8) van een dienstaanbieder, waarbij een activation code (3) in elektronische of magnetische vorm op de elektromagnetische kraskaart (1) aanwezig is en waarbij de activation code (3) gebruikt wordt om een bij de elektromagnetische kraskaart (1) behorende en in de server (8) opgeslagen card balance (13) te activeren.

[fig. 1]

7-11

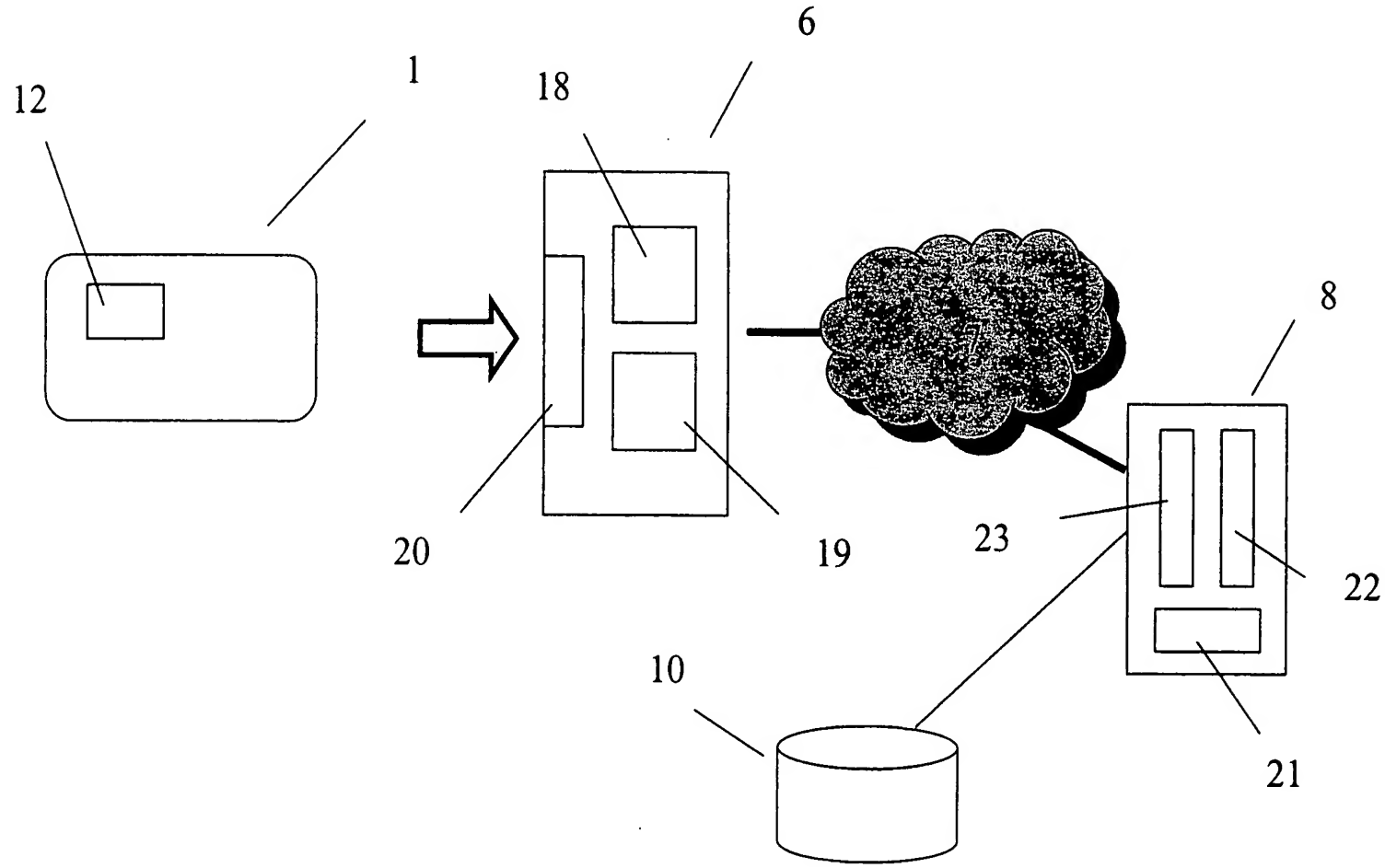


FIG. 1

1024547

WERKWIJZE VOOR HET GEBRUIK VAN EEN ELEKTROMAGNETISCHE KRASKAART VOOR HET LEVEREN VAN DIENSTEN

WERKVELD VAN DE UITVINDING

De uitvinding heeft betrekking op een werkwijze voor het gebruik van een elektromagnetische kraskaart voor het leveren van diensten tussen een voor de dienstafnemer toegankelijke terminal en een tijdens gebruik daarmee verbonden infrastructuur van een dienstaanbieder.

ACHTERGROND VAN DE UITVINDING

Een reeds bekende vooruitbetaalde telefoonkaart is de zogenaamde kraskaart. Hierbij kan de gebruiker een op de kraskaart aanwezige code zichtbaar maken door een beschermende laag weg te krassen. Om het saldo dat de kraskaart vertegenwoordigt te kunnen gebruiken, dient de gebruiker een toegangsnummer van de betreffende dienstaanbieder te kiezen en vervolgens de eerder genoemde code in te toetsen. Vervolgens zal de gebruiker het gewenste b-nummer in moeten toetsen om de telefoonverbinding tot stand te brengen. Het mechanisme voor het afwaarderen van het tegoed op de vooruitbetaalde kraskaart bevindt zich in de infrastructuur van de dienstaanbieder. De werkwijze met behulp van de kraskaart brengt met zich mee dat de gebruiker een lange reeks van nummers in moet toetsen alvorens de telefoonverbinding tot stand te brengen hetgeen als klantonvriendelijk ervaren wordt door de gebruiker.

Een andere reeds bekende werkwijze is beschreven in octrooiaanvrage PCT/EP01/011310 die betrekking heeft op het middels een prepaid chipcard leveren van diensten. Volgens deze werkwijze dient de identiteit en de validiteit van de chipcard vanuit de infrastructuur van de dienstaanbieder te worden geverifieerd alvorens de chipcard te kunnen gebruiken. Deze bekende werkwijze heeft echter als nadeel dat er geen beveiligde procedure wordt gegeven waarmee de verificatie kan worden uitgevoerd.

Een doelstelling van de huidige uitvinding is om de eerder genoemde klantonvriendelijkheid van het gebruik van een kraskaart weg te nemen door de code elektronisch of magnetisch op de kaart te plaatsen. Hiermee ontstaat een

vooruitbetaalde elektronische of magnetische kraskaart, bijvoorbeeld een prepaid chipcard met een elektronische krascode, waardoor het aantal door de gebruiker in te toetsen nummers sterk is gereduceerd. Als de code in elektronische vorm op de chipcard staat, bestaat echter het gevaar dat deze code op een andere chipcard gekopieerd wordt hetgeen fraude in de hand werkt. Een mogelijkheid om de fraude tegen te gaan is de elektronische code door middel van een eenvoudig elektronisch slot te beschermen tegen kopieeracties. Een eenvoudig elektronisch slot biedt echter te weinig afdoende bescherming. Als bekend is hoe van een elektronische kraskaart het slot elektronisch ontgrendeld kan worden, kan de ontgrendeling ook toegepast worden voor alle andere elektronische kraskaarten. Om de elektronische code beter te beschermen is volgens de stand van de techniek echter relatief dure logica op de elektronische kraskaart nodig.

SAMENVATTING VAN DE UITVINDING

Het is een doelstelling van deze uitvinding om de nadelen van de prior art te elimineren en een werkwijze en een systeem te verschaffen waarbij een elektronische of magnetische code op een prepaid card gebruikt wordt om de prepaid card op een beveiligde manier open te krassen zonder dat er relatief dure logica op de prepaid card aanwezig dient te zijn.

Omdat de uitvinding van toepassing is bij zowel elektronische als magnetische kraskaarten, zal, waar van toepassing, worden gesproken van een "elektromagnetische kraskaart", hetgeen verwijst naar elektronische of magnetische opslag van data of beide. Elektronische opslag kan gebeuren in bijvoorbeeld een halfgeleidergeheugen van een chipkaart, terwijl magnetische opslag kan plaatsvinden in een geheugen waarin informatie magnetisch kan worden weggeschreven en uitgelezen.

Daartoe betreft de uitvinding een werkwijze voor het middels een elektromagnetische kraskaart leveren van diensten tussen een voor een dienstafnemer toegankelijke terminal en een infrastructuur, omvattend een netwerk en een server van een dienstaanbieder, waarbij een activation code in elektronische of magnetische vorm op de elektromagnetische kraskaart aanwezig is en waarbij de activation code gebruikt wordt om een bij de elektromagnetische kraskaart behorende en voor de server toegankelijke card balance te activeren.

De aldus gecreëerde elektromagnetische kraskaart kan, in een uitvoeringsvorm, worden geactiveerd zodra een activation code afkomstig van de elektromagnetische kraskaart via een terminal en een netwerk aan een server van een dienstaanbieder wordt aangeboden.

Opgemerkt wordt dat de kraskaart kan worden gebruikt voor diensten van verschillende dienstaanbieders.

Om de activation code van de elektromagnetische kraskaart af te lezen, dient, in een uitvoeringsvorm, eerst een activation challenge behorende bij de elektromagnetische kraskaart aan de elektromagnetische kraskaart te worden aangeboden. Om te verifiëren of de aangeboden activation challenge correct is, wordt de activation challenge vergeleken door middel van eenvoudige logica met een initial challenge die in elektronische of magnetische vorm op de elektromagnetische kraskaart aanwezig is. Indien de activation challenge correct is, dan wordt de activation code vrijgegeven.

Volgens deze uitvinding kan, in een verdere uitvoeringsvorm, de aangeboden activation challenge op de elektromagnetische kraskaart worden vastgelegd. Een result die in elektronische of magnetische vorm op de elektromagnetische kraskaart aanwezig is krijgt door middel van eenvoudige logica op de elektromagnetische kraskaart de waarde van activation code toegekend indien de aangeboden challenge correct is. Indien een incorrecte activation challenge aan de elektromagnetische kraskaart is aangeboden, dan krijgt result een foutcode toegekend. Op deze wijze worden pogingen tot fraude op de elektromagnetische kraskaart vastgelegd. Result wordt via de infrastructuur van de dienstaanbieder naar de server verstuurd, alwaar geverifieerd wordt of result de juiste waarde heeft die nodig is om de elektromagnetische kraskaart te activeren.

Volgens deze uitvinding kan ook de status van de elektromagnetische kraskaart op de elektromagnetische kraskaart worden vastgelegd. Op deze wijze kan worden vastgelegd of de elektromagnetische kraskaart bijvoorbeeld niet-actief, geactiveerd of leeg is.

KORTE BESCHRIJVING VAN DE FIGUREN

Het voorafgaande en de beoogde voordelen van deze uitvinding worden beter inzichtelijk gemaakt aan de hand van de hierna gegeven gedetailleerde beschrijving, wanneer deze tezamen met de begeleidende figuren wordt gelezen, die slechts zijn bedoeld ter illustratie en niet ter beperking van de uitvindingsgedachte waarbij:

FIG. **1** een blokdiagram is waarin een elektronische kraskaart (1) is weergegeven, tezamen met de context waarbinnen de elektronische kraskaart (1) gebruikt wordt.

FIG. **2** een blokdiagram is waarin de opbouw van de elektronische kraskaart (1) is weergegeven.

FIG. **3** een stroomdiagram is waarin de verschillende stappen staan weergegeven die doorlopen worden bij het lezen en activeren van een elektronische kraskaart (1) ten einde gebruik te maken van een dienst van een dienstaanbieder.

FIG. **4** een blokdiagram is waarin de opbouw van database (10) nader is weergegeven.

VERKLARENDE UITVOERINGSVORMEN

Opgemerkt wordt dat de nu volgende figuurbeschrijving betrekking heeft op een elektronische kraskaart, dat wil zeggen een kaart waarin de informatie elektronisch wordt opgeslagen. Zoals gezegd, is de uitvinding hiertoe niet beperkt: informatie kan ook magnetisch zijn opgeslagen. Vandaar dat de conclusies spreken over een "elektromagnetische kraskaart".

FIG. **1** toont een voordelige uitvoeringsvorm van de uitvinding. Een elektronische kraskaart (1) is weergegeven, die bijvoorbeeld een prepaid chipcard is. De term krassen waaraan hier gerefereerd wordt, refereert aan het vrijmaken van een elektronische code die aanwezig is in een elektronisch circuit (12) op de elektronische kraskaart (1) teneinde de elektronische kraskaart (1) te kunnen gebruiken. Een terminal (6) bevat de faciliteiten om de elektronische kraskaart (1) door een gebruiker te laten inbrengen, en om op elektronische wijze gegevens met de elektronische kraskaart uit te wisselen. De terminal (6) omvat een processor (18), een elektronisch opslagmedium (19) en een in- en uitvoerfaciliteit (20). De terminal (6) is gekoppeld aan een infrastructuur (7) van de dienstaanbieder. Deze

koppeling kan op elke geschikte wijze zijn gerealiseerd, zoals bijvoorbeeld middels allerlei soorten vaste verbindingen (koper, glas, etc.) of door middel van een draadloze verbinding. De in de figuur weergegeven infrastructuur (7) is een vaste of mobiele infrastructuur, en is geschikt voor het leveren van telefonie gerelateerde diensten aan gebruikers. Een server (8) is aan de infrastructuur (7) gekoppeld, en kan controle uitoefenen op de wijze waarop telefonie gerelateerde diensten door gebruikers kunnen worden gebruikt. De server (8) is een rekeneenheid met een processor (21), een geheugen (22) en een in- en uitvoerfaciliteit (23). Een database (10) bevat gegevens omtrent elektronische kraskaarten (1).

Om gebruik te kunnen maken van een dienst dient de gebruiker een elektronische kraskaart (1) in een terminal (6) te plaatsen. Voordat de gebruiker daadwerkelijk de elektronische kraskaart (1) kan gebruiken wordt een beveiligde procedure doorlopen om de elektronische kraskaart (1) te activeren. Om de procedure veilig te laten verlopen bevat het elektronische circuit (12) op de elektronische kraskaart (1) een aantal componenten die in FIG. **2** zijn toegelicht.

FIG. **2** toont hoe het elektronische circuit (12) van de elektronische kraskaart (1) is opgebouwd. Het elektronische circuit (12) omvat een elektronisch opslagmedium (15), een processor (16), en een in- en uitvoerfaciliteit (17). Het elektronisch opslagmedium (15) op de elektronische kraskaart (1) omvat een card ID (2). De card ID (2) is bijvoorbeeld een random waarde uit een zeer grote verzameling. Ook omvat het elektronische opslagmedium (15) een activation code (3). De activation code (3) is de code die, via een beveiligde procedure, van de elektronische kraskaart (1) moet worden onttrokken en vervolgens via een netwerk (7) worden aangeboden aan een server (8) om vervolgens de elektronische kraskaart (1) te activeren. Als de elektronische kraskaart (1) geactiveerd is kan de gebruiker gebruik maken van de dienst. De activation code (3) is per elektronische kraskaart (1) anders, en staat op een beveiligde manier op elektronische kraskaart (1). De geheugenlocatie met de activation code (3) kan, nadat de elektronische kraskaart (1) is uitgegeven, alleen worden gelezen. De activation code (3) is vergelijkbaar met de code die op een 'gewone' kraskaart zichtbaar wordt na 'krassen' door de gebruiker.

Om de activation code (3) te beveiligen staat er op de elektronische kraskaart bovendien een initial challenge (4), die, evenals de activation code (3) zelf, is geblokkeerd tegen uitleesacties. Bovendien staan er op de elektronische kraskaart

(1) een challenge (5) en een result (11). De initial challenge (4) is een code die via het netwerk (7) aan de elektronische kraskaart (1) aangeboden moet worden teneinde de activation code (3) aan de elektronische kraskaart (1) te onttrekken en dus de elektronische kraskaart (1) te activeren. De geheugenlocatie met de initial challenge (4) kan, nadat de elektronische kraskaart (1) is uitgegeven, alleen worden gelezen.

Challenge (5) is een code die aangeeft welke waarde aan de elektronische kraskaart (1) is aangeboden met als doel deze te activeren, en waarmee tevens de status van de elektronische kraskaart afgelezen kan worden (niet-actief, actief, leeg) met als initiële waarde C1 (niet-actief). De geheugenlocatie met challenge (5) kan, nadat de elektronische kraskaart (1) is uitgegeven, zowel worden gelezen als geschreven.

In een uitvoeringsvorm is challenge (5) uitgevoerd op de elektronische kraskaart (1) door middel van een PROM (Programmable Read Only Memory). De bits van challenge (5) kunnen alleen van '1' naar '0' worden geschreven en niet meer terug. Dit heeft tot gevolg dat het maximaal aantal pogingen om challenge (5) te 'gokken' beperkt is tot de lengte van challenge (5) in bits minus één. Nadat een fraudeur dit aantal pogingen vruchteloos doorlopen heeft, staat er een foute challenge (5) op de elektronische kraskaart (1), dat wil zeggen een challenge (5) die niet gelijk is aan initial challenge (4). Een voordeel dat deze uitvinding biedt bestaat er uit dat op deze wijze aan challenge (5) is te zien of er een poging tot fraude is gedaan. In een andere uitvoeringsvorm is challenge (5) een groot getal van bijvoorbeeld 64 bits dat onbeperkt geschreven kan worden. Door de grote lengte van challenge (5) is het nagenoeg onmogelijk de juiste challenge (5) te 'gokken', hetgeen als een bescherming tegen fraude fungeert.

In een uitvoeringsvorm is een result (11) op de elektronische kraskaart (1) aanwezig. Result (11) krijgt een waarde toegekend die wordt bepaald door het al dan niet aanbieden van de juiste activation challenge (9) aan de elektronische kraskaart (1).

Aan de hand van een uitvoeringsvorm van de uitvinding wordt de volgende activeringsprocedure doorlopen (zie FIG. **3**). Nadat de gebruiker de elektronische kraskaart (1) in de terminal (6) heeft ingebracht wordt vanuit de terminal (6) een uitleesopdracht naar de elektronische kraskaart (1) verstuurd (stap 1). De

elektronische kraskaart (1) stuurt op basis hiervan de card ID (2) en de challenge (5) naar de terminal (6) (stap 2). Door de terminal wordt de ontvangen challenge (5) vergeleken met een vooraf bepaalde unieke code C1 (bijvoorbeeld '111....1') (stap 3). Als de challenge (5) gelijk is aan C1, betekent dit dat de elektronische kraskaart (1) nog niet geactiveerd is en moet de activeringsprocedure verder worden doorlopen.

In het geval dat de challenge (5) gelijk aan C1 is, wordt door de terminal (6) een verzoek gedaan (stap 4) aan de server (8) om een activation challenge (9) naar de terminal (6) te versturen. Bij dit verzoek wordt de card ID (2) door de terminal (6) meegestuurd. De activation challenge (9) is een code die, mits identiek aan de initial challenge (4) op de elektronische kraskaart (1), bewerkstelligt dat de activation code (3) aan de elektronische kraskaart (1) kan worden onttrokken. De activation challenge (9) staat centraal in een database (10) van de server (8) geregistreerd en is gekoppeld aan de card ID (2).

In FIG. **4** is de database (10) weergegeven. De database (10) is een opslagmedium waarin in elektronische vorm gegevens zijn opgeslagen die voor de server (8) toegankelijk zijn. De database (10) bevat per card ID (2) geheugenlocaties met daarin een activation code check (14), de activation challenge (9), en een card balance (13). De geheugenlocatie behorende bij card ID (2) met de activation code check (14) wordt gebruikt om te verifiëren of de juiste, van de elektronische kraskaart (1) afkomstige, activation code (3) aan de database (10) wordt aangeboden. De geheugenlocatie in de database (10) met de activation challenge (9) behorende bij een elektronische kraskaart (1) is te lezen met als doel deze activation challenge (9), na een request afkomstig van de terminal (6), te kunnen aanbieden aan de elektronische kraskaart (1). In een andere uitvoeringsvorm kan de activation challenge (9) ook afkomstig zijn van een andere bron dan de database (10), bijvoorbeeld van terminal (6). Activation code check (14) en activation challenge (9) kunnen uniek zijn, of kunnen uniek zijn in combinatie met card ID (2).

De geheugenlocatie in de database (10) met card balance (13) behorende bij een card ID (2) is een waarde die aangeeft hoe lang, en additioneel of optioneel in welke mate, een gebruiker gebruik kan maken van diensten door middel van de elektronische kraskaart (1). In een uitvoeringsvorm is de card balance (13) een door de server (8) af te waarderen waarde. Het afwaarderen gebeurt zodra of

zolang er gebruik wordt gemaakt van een dienst. Wanneer de card balance (13) door het afwaarderen een vooraf bepaalde waarde (bijvoorbeeld '0') heeft bereikt, en is het niet meer mogelijk gebruik te maken van diensten middels de betreffende elektronische kraskaart (1).

Volgens deze uitvinding wordt door de server (8) de bij de ontvangen card ID (2) behorende activation challenge (9) opgezocht (stap 5), en wordt de activation challenge (9) verstuurd naar de terminal (6) (stap 6). De terminal (6) verstuurt de activation challenge (9) naar de elektronische kraskaart (1), alwaar de challenge (5) overschreven wordt door de activation challenge (9) (stap 7). Vervolgens stuurt de terminal (6) een verzoek om result (11) te ontvangen (stap 8) naar de elektronische kraskaart (1). Op de elektronische kraskaart (1) wordt de challenge (5), die inmiddels de waarde bevat gelijk aan de eerder van de server (8) ontvangen activation challenge (9), vergeleken met de initial challenge (4). Indien challenge (5) gelijk is aan initial challenge (4), dan wordt aan result (11) de waarde van activation code (3) toegekend. Indien challenge (5) niet gelijk is aan initial challenge (4), dan krijgt result (11) bijvoorbeeld een waarde E1, d.w.z. een foutcode, (bijvoorbeeld '00...0') toegekend. Vervolgens wordt result (11) naar terminal (6) gestuurd (stap 9).

Vervolgens worden card ID (2) en result (11) verstuurd (stap 10) van de terminal (6) naar de server (8). Door de server wordt gecontroleerd of result (11) overeenkomt met de bij de card ID (2) behorende waarde van activation code (3) in de database (10). Is dit het geval, dan wordt de balans behorende bij card ID (2) geactiveerd (stap 11). Is result (11) niet gelijk aan de waarde van activation code (3) in de database (10), dan wordt de balans behorende bij card ID (2) niet geactiveerd.

Alvorens de balans behorende bij de elektronische kraskaart (1) wordt opgevraagd wordt er door de terminal (6) nagegaan of result (11) gelijk is aan E1 (stap 12). Als dit niet het geval is, kan terminal (6) de geactiveerde balans opvragen (stap 13) en kan de gebruiker van de elektronische kraskaart (1) van de gewenste dienst gebruik maken. Indien result (11) wel gelijk is aan E1, dan zal de terminal (6) aan de gebruiker aangeven dat de elektronische kraskaart (1) ongeldig is.

Op het moment dat de elektronische kraskaart (1) opgebruikt is, zal de server (8) dat aan de waarde van card balance (13) herkennen (bijvoorbeeld doordat deze de

waarde '0' heeft), zal er vanuit de server (8) worden aangegeven dat de balans behorende bij elektronische kraskaart (1) opgebruikt is. Challenge (5) krijgt dan door terminal (6) een waarde C2 (bijvoorbeeld '00...0') toegekend. De waarde C2 geeft aan dat de card balance (13) behorende bij de elektronische kraskaart opgebruikt is. Indien de elektronische kraskaart (1) actief en niet leeg is, dan heeft challenge (5) een waarde die niet gelijk is aan C1 of C2, maar een waarde die overeenkomt met de aangeboden activation challenge (9) (of in geval van fraude of een fout een andere waarde). Een voordeel van de uitvinding is dat op deze wijze aan challenge (5) is te zien of de elektronische kraskaart (1) niet-actief, actief of leeg is. Als challenge (5) niet gelijk is aan C1 en ook niet gelijk aan C2, dan kan aan de hand van result (11) bovendien gedetecteerd worden of er een poging tot fraude is gepleegd. Result (11) is in een dergelijk geval gelijk aan E1 hetgeen veroorzaakt wordt door een verschil tussen initial challenge (4) en challenge (5). Dit duidt er op dat er getracht is om met een verkeerde activation challenge (9) de activation code (3) van de elektronische kraskaart (1) te onttrekken.

CONCLUSIES

1. Werkwijze voor het middels een elektromagnetische kraskaart (1) leveren van diensten tussen een voor een dienstafnemer toegankelijke terminal (6) en een infrastructuur, omvattend een netwerk (7) en een server (8) van een dienstaanbieder, waarbij een activation code (3) in elektronische of magnetische vorm op de elektromagnetische kraskaart (1) aanwezig is en waarbij de activation code (3) gebruikt wordt om een bij de elektromagnetische kraskaart (1) behorende en voor de server (8) toegankelijke card balance (13) te activeren.

2. Werkwijze volgens conclusie 1, waarbij een unieke card ID (2) op de elektromagnetische kraskaart (1) in elektronische of magnetische vorm aanwezig is.

3. Werkwijze volgens conclusie 1 of 2, waarbij de activation code (3) kan worden uitgelezen door een activation challenge (9) aan de elektromagnetische kraskaart (1) aan te bieden, waarbij de activation challenge (9) gelijk moet zijn aan een initial challenge (4) die in elektronische of magnetische vorm op de elektromagnetische kraskaart (1) aanwezig is.

4. Werkwijze volgens conclusie 3, waarbij een in elektronische of magnetische vorm aanwezige result (11) gebruikt wordt om weer te geven of de aan de elektromagnetische kraskaart (1) aangeboden activation challenge (9) gelijk is aan de op de elektromagnetische kraskaart (1) aanwezige initial challenge (4).

5. Werkwijze volgens conclusie 4, waarbij de card ID (2) en het result (11) via het netwerk (7) worden ontvangen door de server (8), en door de server (8) wordt geverifieerd of het result (11) overeenkomt met de bij de card ID (2) behorende activation code check (14) in een database (10), welke activation code check (14) gelijk is aan de activation code (3) op de elektromagnetische kraskaart (1).

6. Werkwijze volgens conclusie 5, waarbij de card ID (2) en de daarbij horende activation challenge (9), activation code check (14) en een af te waarderen card

balance (13) zich bevinden in de database (10) die toegankelijk is door de server (8).

7. Werkwijze volgens elk van de conclusies 4-6, waarbij het result (11) dezelfde waarde als activation code (3) krijgt indien aan de elektromagnetische kraskaart (1) de juiste activation challenge (9) is aangeboden, en anders een foutcode E1 toegekend krijgt.

8. Werkwijze volgens conclusie 7, waarbij het result (11) door de terminal (6) kan worden uitgelezen en geverifieerd, en waarbij de terminal (6) een melding geeft in het geval het result (11) overeenkomt met de foutcode E1.

9. Werkwijze volgens elk van de conclusies 3-8, waarbij er een challenge (5) op de elektromagnetische kraskaart (1) in elektronische of magnetische vorm aanwezig is, die de status van de elektromagnetische kraskaart (1) weergeeft en de waarde toegekend kan krijgen van de aan de elektromagnetische kraskaart (1) aangeboden activation challenge (9).

10. Werkwijze volgens conclusie 9, waarbij de challenge (5) door de terminal (6) wordt uitgelezen ten einde de status van de elektromagnetische kraskaart (1) vast te stellen.

11. Werkwijze volgens conclusies 9 of 10, waarbij de challenge (5) op een waarde C2 wordt gezet indien de card balance (13) bij card ID (2) verbruikt is.

12. Werkwijze volgens elk van de conclusies 3-11, waarbij de aan de elektromagnetische kraskaart (1) aangeboden activation challenge (9) op de elektromagnetische kraskaart (1) wordt opgeslagen.

13. Werkwijze volgens elk van de conclusies 3-12, waarbij de activation challenge (9) afkomstig is van de server (8).

14. Een elektromagnetische kraskaart (1) ingericht voor het verschaffen van diensten aan een dienstafnemer via een terminal (6) en een, een netwerk (7) en een server (8) omvattende infrastructuur van een dienstaanbieder, waarbij de elektromagnetische kraskaart is voorzien van een processor (12), een met de processor verbonden geheugen (15) en een met de processor verbonden

invoer/uitvoereenheid (17) voor communicatie met de terminal, waarbij een activation code (3) in het geheugen (15) is opgeslagen, en de processor (16) is ingericht om via communicatie met de server en met gebruik van de activation code (3) een bij de elektromagnetische kraskaart (1) behorende en voor de server (8) toegankelijke card balance (13) te activeren.

15. Een elektromagnetische kraskaart (1) volgens conclusie 14, waarbij in het geheugen tevens een unieke card ID (2) en een initial challenge (4) zijn opgeslagen, en de processor is ingericht om de activation code (3) uit te lezen na ontvangst van een activation challenge (9), waarbij de activation challenge (9) gelijk moet zijn aan de initial challenge (4).

16. Een elektromagnetische kraskaart (1) volgens conclusie 15, waarbij de processor is ingericht om een result (11) in het geheugen op te slaan, welke gebruikt wordt om weer te geven of de aan de elektromagnetische kraskaart (1) aangeboden activation challenge (9) gelijk is aan de op de elektromagnetische kraskaart (1) aanwezige initial challenge (4).

17. Een elektromagnetische kraskaart (1) volgens conclusies 15-16, waarbij in het geheugen tevens een challenge (5) is opgeslagen, die de status van de elektromagnetische kraskaart (1) weergeeft en de processor is ingericht om de challenge (5) de waarde toe te kennen van de aan de elektromagnetische kraskaart (1) aangeboden activation challenge (9).

18. Een terminal (6) die is aangesloten aan een infrastructuur omvattende een netwerk (7) en een server (8) van een dienstaanbieder, waarbij de terminal is voorzien van een terminal processor (18) en terminal invoer/uitvoermiddelen (20) om te communiceren met een elektromagnetische kraskaart volgens een van de voorgaande conclusies, welke terminal processor (18) is ingericht om van de elektromagnetische kraskaart (1) ontvangen elektronische of magnetische gegevens via het netwerk (7) te versturen naar de server (8), en om van de server (8) ontvangen elektronische of magnetische gegevens te versturen naar de elektromagnetische kraskaart (1) en om een op de elektromagnetische kraskaart (1) aanwezige challenge (5) uit te lezen ten einde de status van de elektromagnetische kraskaart (1) vast te stellen.

19. Een server (8) die is aangesloten op een niet direct voor een dienstafnemer toegankelijke infrastructuur omvattende een netwerk (7) van een dienstaanbieder, en is aangesloten op een database (10), welke server (8) is ingericht om:
- via het netwerk (7) elektronische of magnetische gegevens te ontvangen van een terminal (6),
- de van de terminal (6) ontvangen elektronische of magnetische gegevens te vergelijken met elektronische of magnetische gegevens in de database (10),
- op basis van elektronische of magnetische gegevens die van de terminal (6) ontvangen zijn elektronische of magnetische gegevens uit de database (10) op te vragen en via het netwerk (7) te versturen naar de terminal (6),
- op basis van elektronische of magnetische gegevens die van de terminal (6) ontvangen zijn elektronische of magnetische gegevens in de database (10) te wijzigen,
- een bij een card ID (2) behorende activation challenge (9) uit de database (10) op te vragen en via het netwerk (7) te versturen naar de terminal (6), welke card ID (2) via de terminal is ontvangen op unieke wijze een elektromagnetische kraskaart definieert.

20. Een server (8) volgens conclusie19, waarbij de server (8) is ingericht om een card balance (13) in de database (10) af te waarderen in afhankelijkheid van een aan de gebruiker van de elektromagnetische kraskaart verschafte dienst.

******

1024547

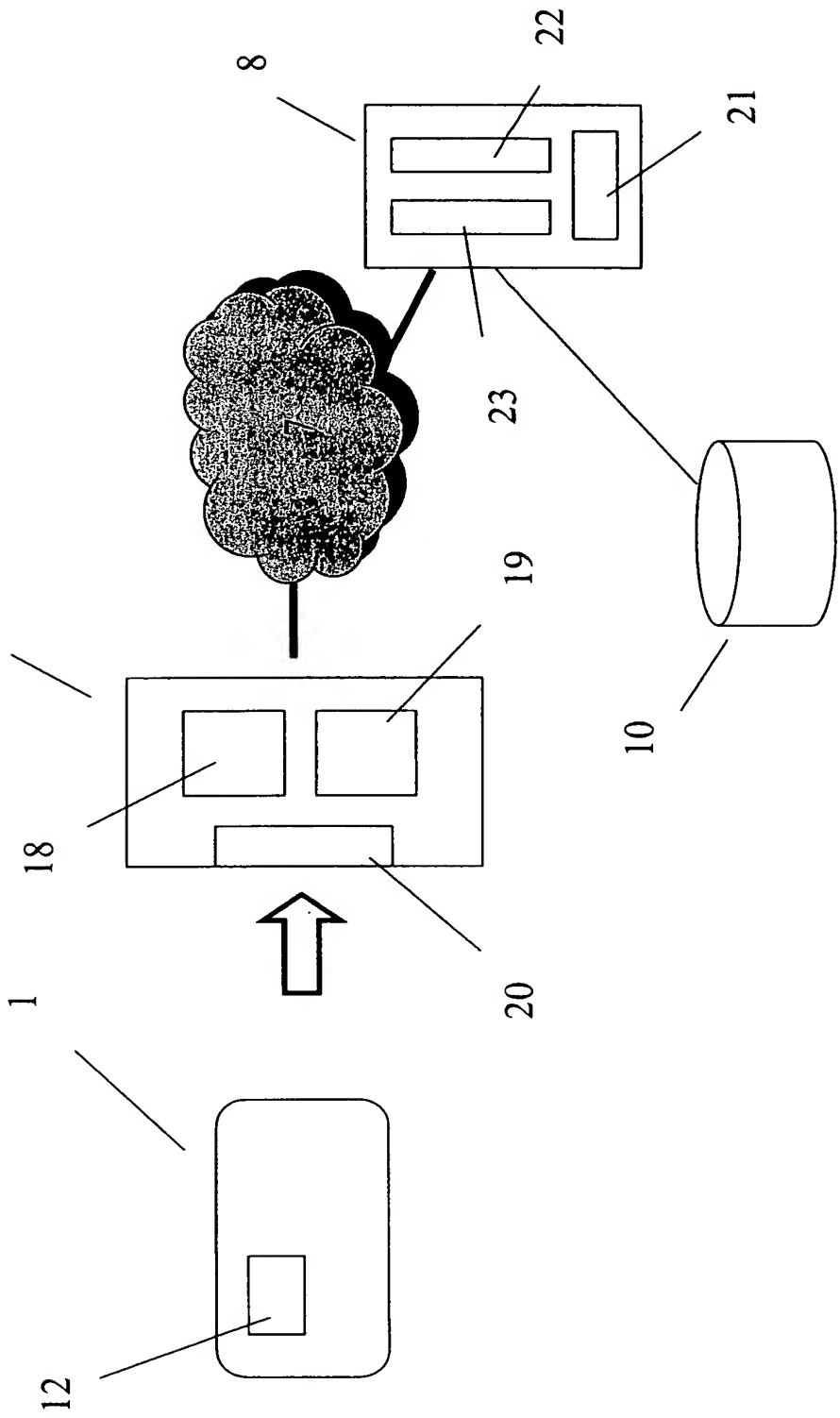


FIG. 1

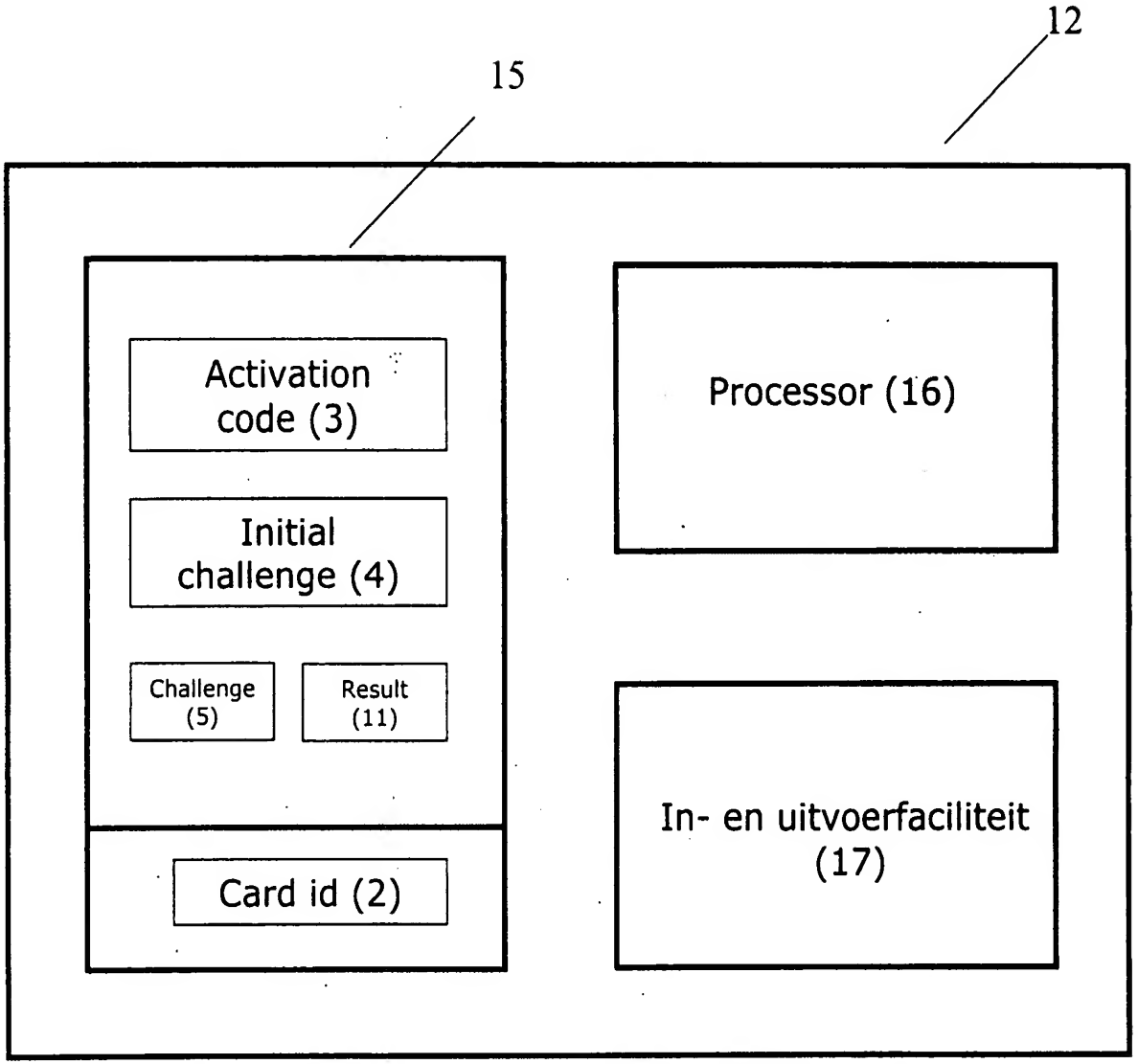

12
15
Activation code (3)
Initial challenge (4)
Challenge (5)
Result (11)
Card id (2)
Processor (16)
In- en uitvoerfaciliteit (17)

FIG. 2

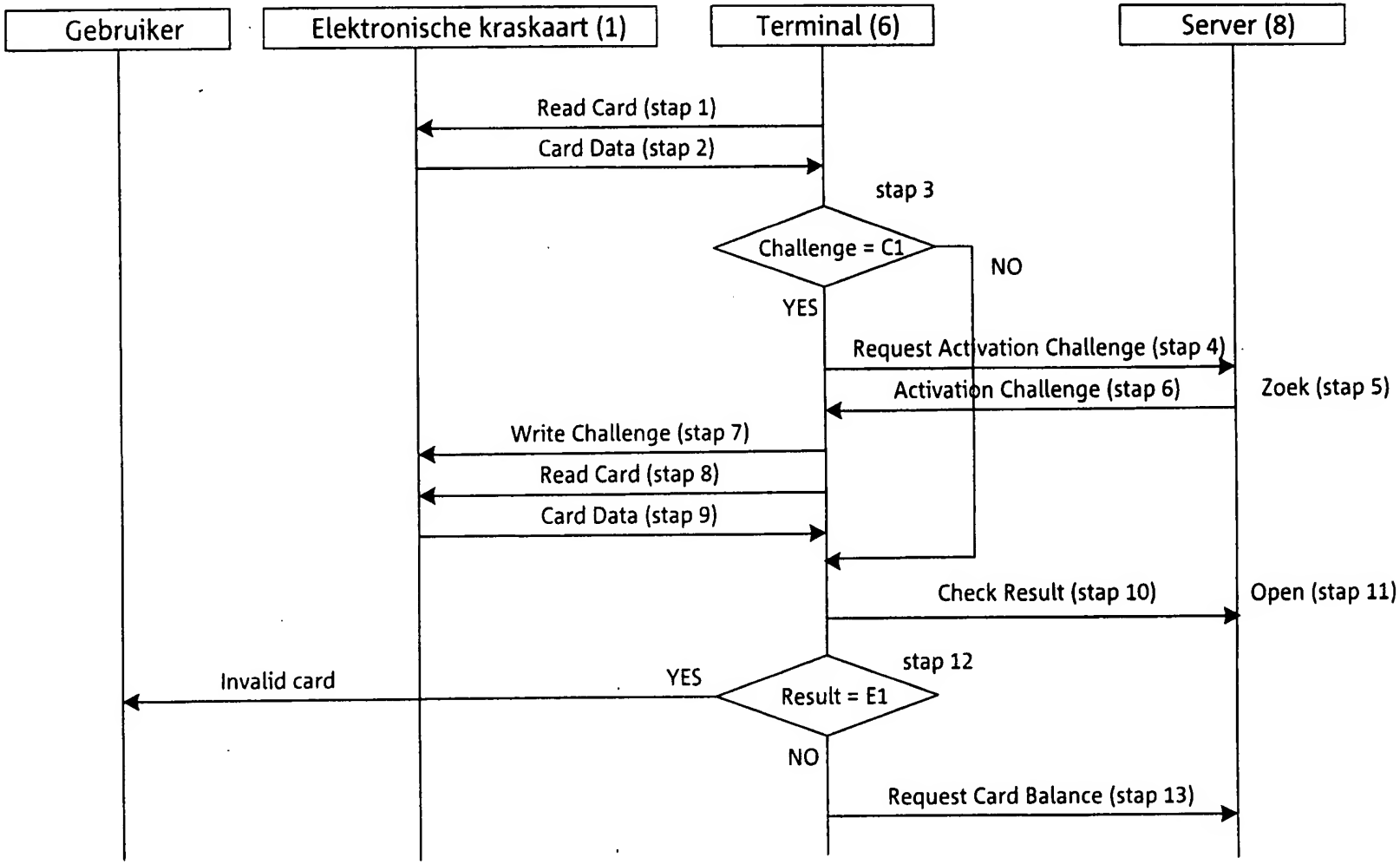

Gebruiker
Elektronische kraskaart (1)
Terminal (6)
Server (8)
Read Card (stap 1)
Card Data (stap 2)
stap 3
Challenge = C1
NO
YES
Request Activation Challenge (stap 4)
Activation Challenge (stap 6)
Zoek (stap 5)
Write Challenge (stap 7)
Read Card (stap 8)
Card Data (stap 9)
Check Result (stap 10)
Open (stap 11)
stap 12
Invalid card
YES
Result = E1
NO
Request Card Balance (stap 13)

FIG. 3

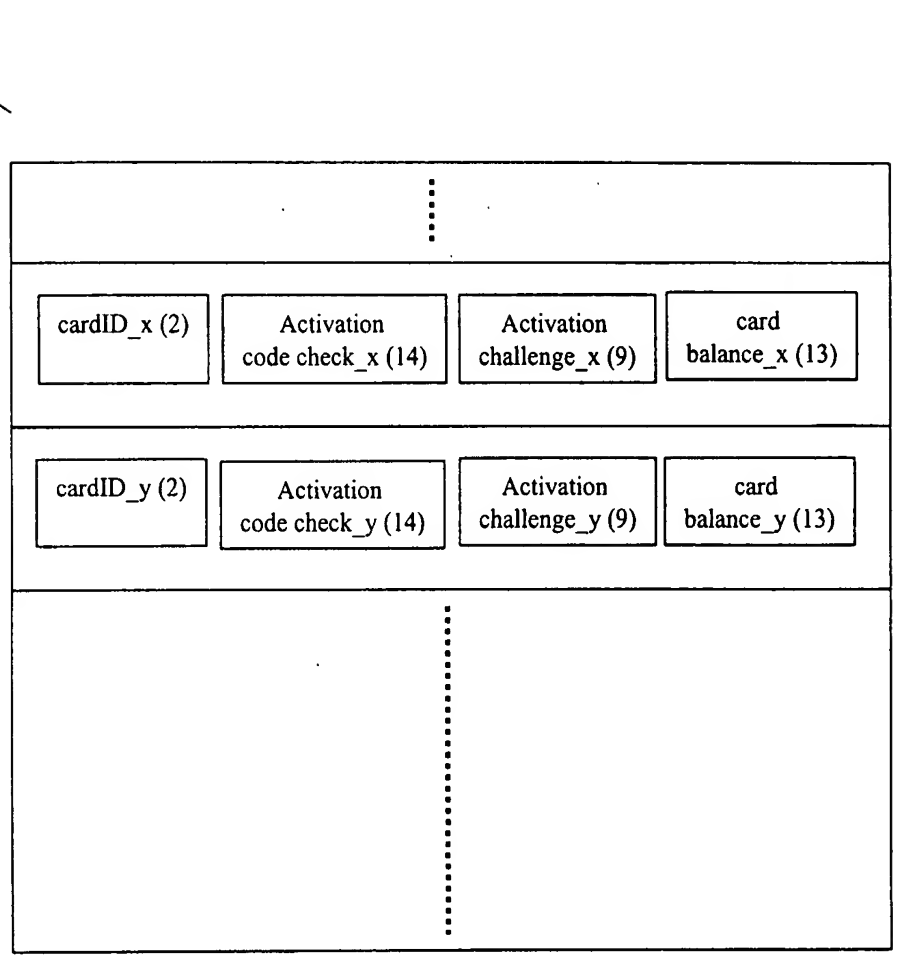

10
cardID_x (2)
Activation code check_x (14)
Activation challenge_x (9)
card balance_x (13)
cardID_y (2)
Activation code check_y (14)
Activation challenge_y (9)
card balance_y (13)

FIG. 4

KINGDOM OF THE (crest) NETHERLANDS

PATENT OFFICE

This certifies that in the Netherlands, on 16 October 2003, a patent application was filed under number 1024547, in the name of:

Koninklijke KPN N.V.

of Groningen

for: " METHOD FOR USING AN ELECTROMAGNETIC SCRATCHCARD TO PROVIDE SERVICES".

claiming priority of the patent application which was filed in the Netherlands on 31 March 2003 under number 1023058, and that the documents attached hereto are in accordance with the documents originally filed.

Rijswijk, 27 January 2004

On behalf of the Chairman of the Patent Office,

(signature)

Mw. M.M. Enhus

ABSTRACT

The invention pertains to a system and a method for using an electromagnetic scratchcard (1) to provide services between a terminal (6) accessible to a service customer and an infrastructure. The system comprises a network (7) and a server (8) of a service provider, whereby an activation code (3) is present in electronic or magnetic form on the electromagnetic scratchcard (1) and whereby the activation code (3) is used to activate a card balance (13) that is associated with the electromagnetic scratchcard (1) and is stored in the server (8).

[FIG. 1].

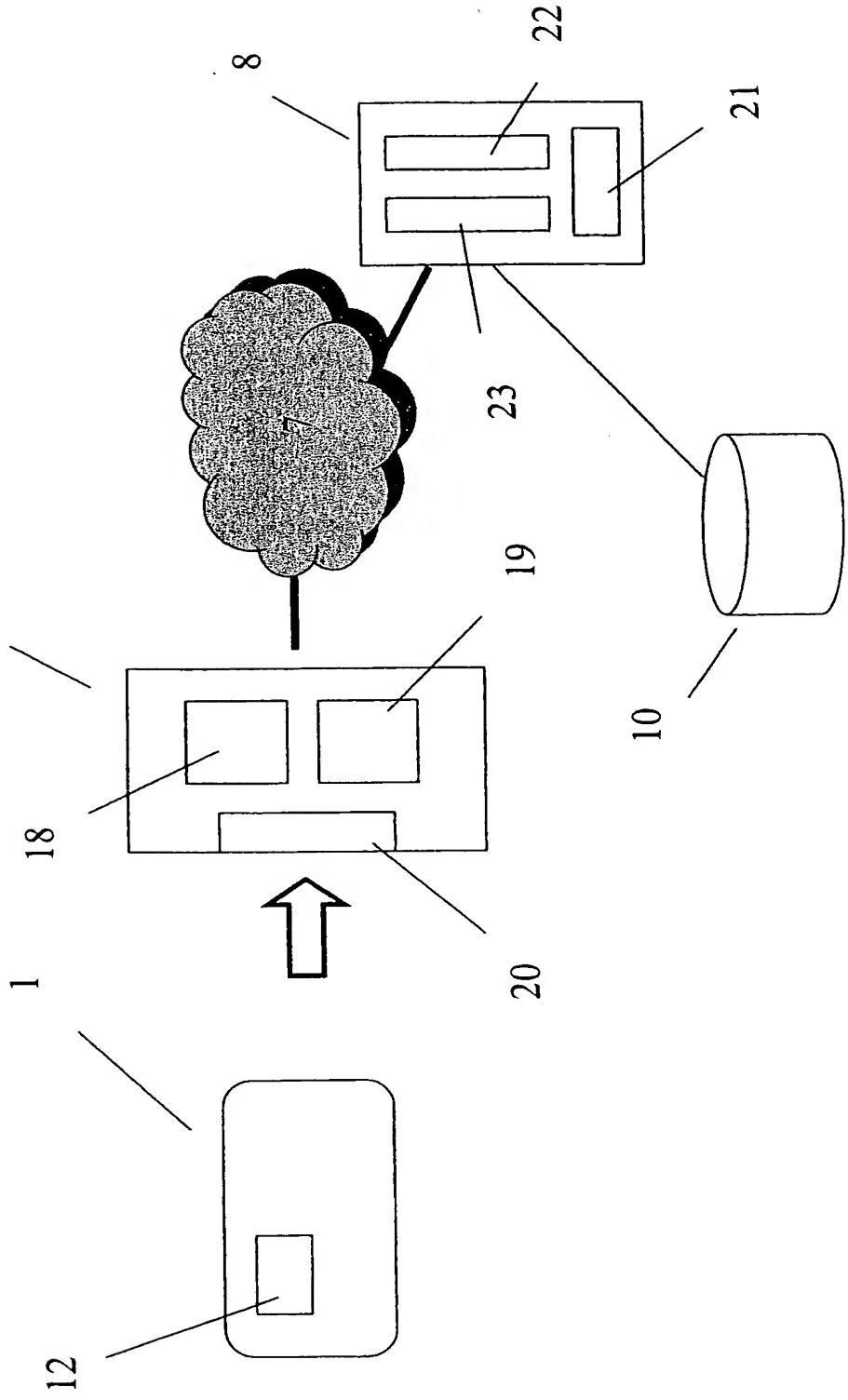


FIG. 1

METHOD FOR USING AN ELECTROMAGNETIC SCRATCHCARD TO PROVIDE SERVICES

SCOPE OF THE INVENTION

The invention pertains to a method for using an electromagnetic scratchcard to provide services between a terminal that is accessible to the service customer and a service provider's infrastructure that is connected to the aforementioned terminal during usage.

BACKGROUND OF THE INVENTION

A known prepaid phonecard is the so-called scratchcard. By scratching away a protective layer, the user can make visible a code present on the scratchcard. To use the balance that the scratchcard represents, the user must dial an access number of the service provider and then enter the aforementioned code. Subsequently, the user must dial the required "B" number to set up the telephone connection. The mechanism for reducing the balance on the prepaid scratchcard is located in the service provider's infrastructure. The method using the scratchcard requires the user to key in a long series of numbers in order to set up the telephone connection, which the user experiences as user-unfriendly.

Another known method is described in patent application PCT/EP01/011310 that pertains to providing services by means of a prepaid chipcard. According to that method, the identity and validity of the chipcard must be verified from within the service provider's infrastructure before it is possible to use the chipcard. A disadvantage of this known method, however, is that it does not provide a secure procedure for executing verification.

An objective of the present invention is to eliminate the aforementioned customer-unfriendliness by placing the code electronically or magnetically on the card. This creates a prepaid electronic or magnetic scratchcard, for example a prepaid chipcard with an electronic scratch code, thus greatly reducing the string of numbers the user must key in. If the code occurs on a chipcard in electronic form, however, a danger exists that the code will be copied to another chipcard, thus facilitating fraudulent use. A possibility for combating fraud is to use a simple

electronic lock to protect the electronic code against copying attempts. However, a simple electronic lock provides insufficient proper protection. Knowledge of how to unlock an electronic scratchcard's lock means the same unlocking will be usable for all other electronic scratchcards. To improve protection of the electronic code, relatively expensive logics are required on the electronic scratchcard according to the state of the art.

SUMMARY OF THE INVENTION

An objective of the present invention is to eliminate the disadvantages of the prior art and to provide a method and a system enabling an electronic or magnetic code on a prepaid card to be used to scratch open the prepaid card securely, without the need for relatively expensive logics to be present on the prepaid card.

As the invention applies both to electronic and to magnetic scratchcards, this document refers, where applicable, to an "electromagnetic scratchcard", which refers to electronic or magnetic data storage, or both. Electronic storage can take place in, for example, a semiconductor memory of the chipcard, while magnetic storage can take place in a memory in which information can be copied and read magnetically.

For this purpose, the invention embodies a method for using an electromagnetic scratchcard to provide services between a terminal accessible to a service user and an infrastructure that comprises a network and a server of a service provider, whereby an activation code is present in electronic or magnetic form on the electromagnetic scratchcard and whereby the activation code is used to activate a card balance that is associated with the electromagnetic scratchcard and is accessible to the server.

The electromagnetic scratchcard thus created can, in one embodiment, be activated as soon as an activation code originating from the electromagnetic scratchcard is offered to a service provider's server via a terminal and a network.

It should be noted that the scratchcard is usable for services from various service providers.

To read out the activation code from the electromagnetic scratchcard, it is first necessary, in one embodiment, to offer to the electromagnetic scratchcard an activation challenge associated with the electromagnetic scratchcard. To verify whether the offered activation challenge is correct, the activation challenge is compared, by means of simple logics, with an initial challenge present on the electromagnetic scratchcard in electronic or magnetic form. If the activation challenge is correct, the activation code will be released.

According to this invention, the offered activation challenge can, in a further embodiment, be stored on the electromagnetic scratchcard. A result present in electronic or magnetic form on the electromagnetic scratchcard will be assigned the value of the activation code, by means of simple logics on the electromagnetic scratchcard, provided that the offered challenge is correct. If an incorrect activation challenge is offered to the electromagnetic scratchcard, the result will be assigned an error code. In this way, instances of attempted fraud will be recorded on the electromagnetic scratchcard. The result will be sent via the service provider's infrastructure to the server where verification will occur of whether the result has the correct value necessary to activate the electromagnetic scratchcard.

According to this invention, the status of the electromagnetic scratchcard can also be recorded on the electromagnetic scratchcard. In this way, it is possible to record whether the electromagnetic scratchcard is, for example, non-active, activated or empty.

BRIEF DESCRIPTION OF THE FIGURES

The foregoing and the envisaged advantages of this invention will be further clarified by reading the detailed description given below in conjunction with examination of the accompanying figures, which are intended solely for illustration and not for limitation of the principle of the invention, whereby:

FIG. **1** is a block diagram that shows an electronic scratchcard (1) together with the context in which the electronic scratchcard (1) will be used.

FIG. **2** is a block diagram that shows the structure of the electronic scratchcard (1).

FIG. **3** is a flow diagram that shows the different steps that occur during reading and activation of an electronic scratchcard (1) to be able to use a service offered by a service provider.

FIG. **4** is a block diagram that shows the structure of the database (10) in more detail.

EXPLANATORY EMBODIMENTS

It should be noted that the figure descriptions given below pertain to an electronic scratchcard, i.e. a card in which information is stored electronically. As mentioned earlier, the invention is not confined to this particular embodiment, because information is also storable magnetically. This is the reason why the claims refer to an "electromagnetic scratchcard".

FIG. **1** shows an advantageous embodiment of the invention. The shown electronic scratchcard (1) is, for example, a prepaid chipcard. The term scratching as employed here refers to the release of an electronic code present in an electronic circuit (12) on the electronic scratchcard (1) in order to use the electronic scratchcard (1). A terminal (6) contains the facilities that allow a user to insert the facilities on the electronic scratchcard (1) and to exchange data electronically with the electronic scratchcard. The terminal (6) comprises a processor (18), an electronic storage medium (19) and an input and output device (20). The terminal (6) is connected to an infrastructure (7) of the service provider. This connection may have been created in any suitable way, for example by such means as all kinds of leased lines (copper-wire, fiber-optic, etc) or by means of a wireless connection. The infrastructure (7) shown in the figure is a fixed or mobile infrastructure that is suitable for providing telephony-related services to users. A server (8) is connected to the infrastructure (7) and can exercise control over the way users are able to use telephony-related services. The server (8) is a computing unit with a processor (21), a memory (22) and an input and output device (23). A database (10) contains data concerning electronic scratchcards (1).

To be able to use the service, the user must insert an electronic scratchcard (1) in a terminal (6). Before the user can actually use the electronic scratchcard (1), a secure procedure is run to activate the electronic scratchcard (1). To allow the

procedure to take place securely, the electronic circuit (12) on the electronic scratchcard (1) contains several components that are explained in FIG. 2.

FIG. **2** shows how the electronic circuit (12) of the electronic scratchcard (1) is structured. The electronic circuit (12) contains an electronic storage medium (15), a processor (16) and an input and output device (17). The electronic storage medium (15) on the electronic scratchcard (1) contains a card ID (2). The card ID (2) is, for example, a random value from a very large set. The electronic storage medium (15) further contains an activation code (3). The activation code (3) is the code that, through a secure procedure, must be derived from the electronic scratchcard (1) and then offered, via a network (7), to a server (8) so as subsequently to activate the electronic scratchcard (1). If the electronic scratchcard (1) has been activated, the user will be able to use the service. The activation code (3) is different for each electronic scratchcard (1) and is held in a secure way on the electronic scratchcard (1). After the electronic scratchcard (1) has been issued, the memory location with the activation code (3) can be read only. The activation code (3) is similar to the code that becomes visible on an "ordinary" scratchcard after "scratching" by the user.

To make the activation code (3) secure, the electronic scratchcard additionally contains an initial challenge (4) that, like the activation code (3) itself, is blocked to prevent read-out actions. Moreover, the electronic scratchcard (1) contains a challenge (5) and a result (11). The initial challenge (4) is a code that must be offered, via the network (7), to the electronic scratchcard (1) in order to derive the activation code (3) from the electronic scratchcard (1) and thus activate the electronic scratchcard (1). After the electronic scratchcard (1) has been issued, the memory location containing the initial challenge (4) can be read only.

The challenge (5) is a code that indicates the value that has been offered to the electronic scratchcard (1) for the purpose of activating the card, and by means of which it is further possible to read out the status of the electronic scratchcard (non-active, active, empty), whereby the initial value is C1 (non-active). After the electronic scratchcard (1) has been issued, the memory location with the challenge (5) is capable of being read and written.

In one embodiment, the challenge (5) is placed on the electronic scratchcard (1) by means of a PROM (Programmable Read Only Memory). The bits of the challenge (5)

are writable only from "1" to "0" and not back. The consequence of this is that the maximum number of attempts to "guess" the challenge (5) is limited to the length of the challenge (5) in bits minus one. After a fraudulent person has fruitlessly exhausted the number of attempts, there will be an incorrect challenge (5) on the electronic scratchcard (1), i.e. a challenge (5) that is not equal to the initial challenge (4). An advantage of this invention is that, in this way, it can be seen from the challenge (5) whether an attempt of fraudulent usage has occurred. In another embodiment, the challenge (5) is a large number of, say, 64 bits that is writable without limitation. Because of the large length of the challenge (5), it is virtually impossible to "guess" the correct challenge (5), a circumstance affording protection against fraud.

In one embodiment, a result (11) is present on the electronic scratchcard (1). The result (11) is assigned a value that is determined by whether or not the correct activation challenge (9) is offered to the electronic scratchcard (1).

Using an embodiment of the invention, the activation procedure will be carried out (see FIG. **3**). After the user has inserted the electronic scratchcard (1) in the terminal (6), a read-out instruction is sent from the terminal (6) to the electronic scratchcard (1) (step 1). The electronic scratchcard (1) responds by sending the card ID (2) and the challenge (5) to the terminal (step 2). The terminal compares the received challenge (5) with a predetermined unique code C (for example "111... 1") (step 3). If the challenge (5) is equal to C1, it means that the electronic scratchcard (1) has not yet been activated and the activation procedure must be continued further.

If the challenge (5) is equal to C1, the terminal (6) will request (step 4) the server (8) to send an activation challenge (9) to the terminal (6). Together with this request, the terminal (6) will send the card ID (2). The activation challenge (9) is a code that, provided it is identical to the initial challenge (4) on the electronic scratchcard (1), enables the activation code (3) to be derived from the electronic scratchcard (1). The activation challenge (9) is recorded centrally in a database (10) of the server (8) and is linked to the card ID (2).

FIG. **4** shows the database (10). The database (10) is a storage medium with electronically stored data that are accessible to the server (8). For each card ID (2), the database (10) contains memory locations within which there is an activation

code check (14), the activation challenge (9) and a card balance (13). The memory location associated with the card ID (2) with the activation code check (14) is used to verify whether the correct activation code (3) originating from the scratchcard (1) is being offered to the database (10). The database (10) memory location containing the activation challenge (9) associated with an electronic scratchcard (1) is readable for the purpose of offering the activation challenge (9) to the electronic scratchcard (1) in response to a request originating from the terminal (6). In another embodiment, the activation challenge (9) may also originate from a source other than the database (10), for example from the terminal (6). The activation code check (14) and the activation challenge (9) can be unique, or can be unique in combination with the card ID (2).

The database (10) memory location that contains the card balance (13) associated with a card ID (2) is a value that indicates how long, and additionally or optionally to what extent, a user may use services by means of the electronic scratchcard (1). In one embodiment, the card balance (13) is a value that is reducible by the server (8). Reduction occurs at such time or for as long as use is made of the service. When reduction has caused the card balance (13) to reach a predefined value (for example, "0"), it will cease to be possible to use the services by means of the electronic scratchcard (1) in question.

According to this invention, the server (8) finds the activation challenge (9) associated with the received card ID (2) (step 5), and the activation challenge (9) is sent to the terminal (6) (step 6). The terminal (6) sends the activation challenge (9) to the electronic scratchcard (1), where the challenge (5) is overwritten by the activation challenge (9) (step 7). The terminal (6) then sends to the electronic scratchcard (1) a request to receive a result (11) (step 8). On the electronic scratchcard (1), the challenge (5), which in the meantime contains a value equal to the activation challenge (9) received earlier from the server (8), is compared with the initial challenge (4). If the challenge (5) is equal to the initial challenge (4), the value of the activation code (3) will be assigned to the result (11). If the challenge (5) is unequal to the initial challenge (4), the result (11) will be given a value of, for example, E1, which represents an error code (for example "00..0"). The result (11) will then be sent to the terminal (6) (step 9).

Subsequently, the card ID (2) and result (11) will be sent (step 10) from the terminal (6) to the server (8). The server checks whether the result (11)

corresponds with the value of the activation code (3) in the database (10) that is associated with the card ID (2). If this is the case, the balance associated with the card ID (2) will be activated (step 11). If the result is unequal to the value of the activation code (3) in the database (10), the balance associated with the card ID (2) will not be activated.

Before the balance associated with the electronic scratchcard (1) is retrieved, the terminal (6) will check whether the result (11) is equal to E1 (step 12). If this is not the case, the terminal (6) can retrieve the activated balance (step 13) and the user of the electronic scratchcard (1) will be able to use the desired service. If the result (11) is equal to E1, however, the terminal (6) will inform the user that the electronic scratchcard (1) is invalid.

As such time as the electronic scratchcard (1) becomes exhausted, the server (8) will recognize this circumstance from the value of the card balance (13) (for example, because it has the value "0"), and the server (8) will indicate that the balance associated with the electronic scratchcard (1) has been exhausted. The terminal (6) will then give the challenge (5) a value of C2 (for example, "00... 0"). This value C2 indicates that the card balance (13) associated with the electronic scratchcard has been exhausted. If the electronic scratchcard (1) is active and not empty, the challenge (5) will have a value that is not equal to C1 or C2, but a value that corresponds with the offered activation challenge (9) (or, in the case of fraudulent use or an error, a different value). An advantage of the invention is that, in this way, it can be seen from the challenge (5) whether the electronic scratchcard (1) is non-active, active or empty. If the challenge (5) is not equal either to C1 or to C2, it is moreover possible to detect from the result (11) whether there has been an attempt of fraudulent usage. In such a case, the result (11) will be equal to E1, which is caused by a difference between the initial challenge (4) and the challenge (5). This indicates that an attempt has been made to obtain the activation code (3) from the electronic scratchcard (1) using an incorrect activation challenge (9).

CLAIMS

1. Method for using an electromagnetic scratchcard (1) to provide services between a terminal (6) accessible to a service customer and an infrastructure comprising a network (7) and a server (8) of a service provider, whereby an activation code (3) is present in electronic or magnetic form on the electromagnetic scratchcard (1) and the activation code (3) is used to activate a card balance (13) that is associated with the electromagnetic scratchcard (1) and is accessible to the server (8).

2. Method according to claim 1, whereby a unique card ID (2) in electronic or magnetic form is present on the electromagnetic scratchcard (1).

3. Method according to claim 1 or 2, whereby the activation code (3) can be read out by offering an activation challenge (9) to the electromagnetic scratchcard (1), whereby the activation challenge (9) must be equal to an initial challenge (4) that is present in electronic or magnetic form on the electromagnetic scratchcard (1).

4. Method according to claim 3, whereby a result (11) present in electronic or magnetic form is used to show whether the activation challenge (9) offered to the electromagnetic scratchcard (1) is equal to the initial challenge (4) present on the electromagnetic scratchcard (1).

5. Method according to claim 4, whereby the card ID (2) and the result (11) are received by the server (8) via the network (7), and the server (8) verifies whether the result (11) corresponds with the activation code (3) associated with the card ID (2) in a database (10), such activation code check (14) being equal to the activation code (3) on the electromagnetic scratchcard (1).

6. Method according to claim 5, whereby the card ID (2) and the associated activation challenge (9), activation code check (14) and a reducible card balance (13) are located in the database (10) accessible by the server (8).

7. Method according to one of the claims 4 through 6, whereby the result (11) is given the same value as the activation code (3) if the correct activation challenge

(9) has been offered to the electromagnetic scratchcard (1), or otherwise is given an error code E1.

8. Method according to claim 7, whereby the terminal (6) can read out and verify the result (11), and whereby the terminal (6) gives a report if the result (11) corresponds with the error code E1.

9. Method according to one of the claims 3 through 8, whereby a challenge (5) present in electronic or magnetic form on the electromagnetic scratchcard (1) shows the status of the electromagnetic scratchcard (1) and can be given the value of the activation challenge (9) offered to the electromagnetic scratchcard (1).

10. Method according to claim 9, whereby the terminal (6) reads out the challenge (5) in order to determine the status of the electromagnetic scratchcard (1).

11. Method according to claim 9 or 10, whereby the challenge (5) is set to a value C2 if the card balance (13) for the card ID (2) has been used up.

12. Method according to one of the claims 3 through 11, whereby the activation challenge (9) offered to the electromagnetic scratchcard (1) is stored on the electromagnetic scratchcard (1).

13. Method according to one of the claims 3 through 12, whereby the activation challenge (9) originates from the server (8).

14. An electromagnetic scratchcard (1) arranged to provide services to a service customer by means of a terminal (6) via a service provider's infrastructure comprising a network (7) and a server (8), whereby the electromagnetic scratchcard is provided with a processor (12), a memory (15) connected to the processor and an input/output unit (17) connected to the processor and used for communication with the terminal, whereby an activation code (3) is stored in the memory (15), and the processor (16) is arranged to activate a card balance (13) that is associated with the electromagnetic scratchcard (1) and that is accessible to the server (8), by means of communication with the server and use of the activation code (3).

15. An electromagnetic scratchcard (1) according to claim 14, whereby a unique card ID (2) and an initial challenge (4) are also stored in the memory, and the processor is arranged to read out the activation code (3) after receiving an activation challenge (9), whereby the activation challenge (9) must be equal to the initial challenge (4).

16. An electromagnetic scratchcard (1) according to claim 15, whereby the processor is arranged to store a result (11) in the memory, such result showing whether the activation challenge (9) offered to the electromagnetic scratchcard (1) is equal to the initial challenge (4) present on the electromagnetic scratchcard (1).

17. An electromagnetic scratchcard (1) according to claims 15 and 16, whereby a challenge (5) is also stored in the memory, such challenge showing the status of the electromagnetic scratchcard (1) and being arranged to give the challenge (5) the value of the activation challenge (9) offered to the electromagnetic scratchcard (1).

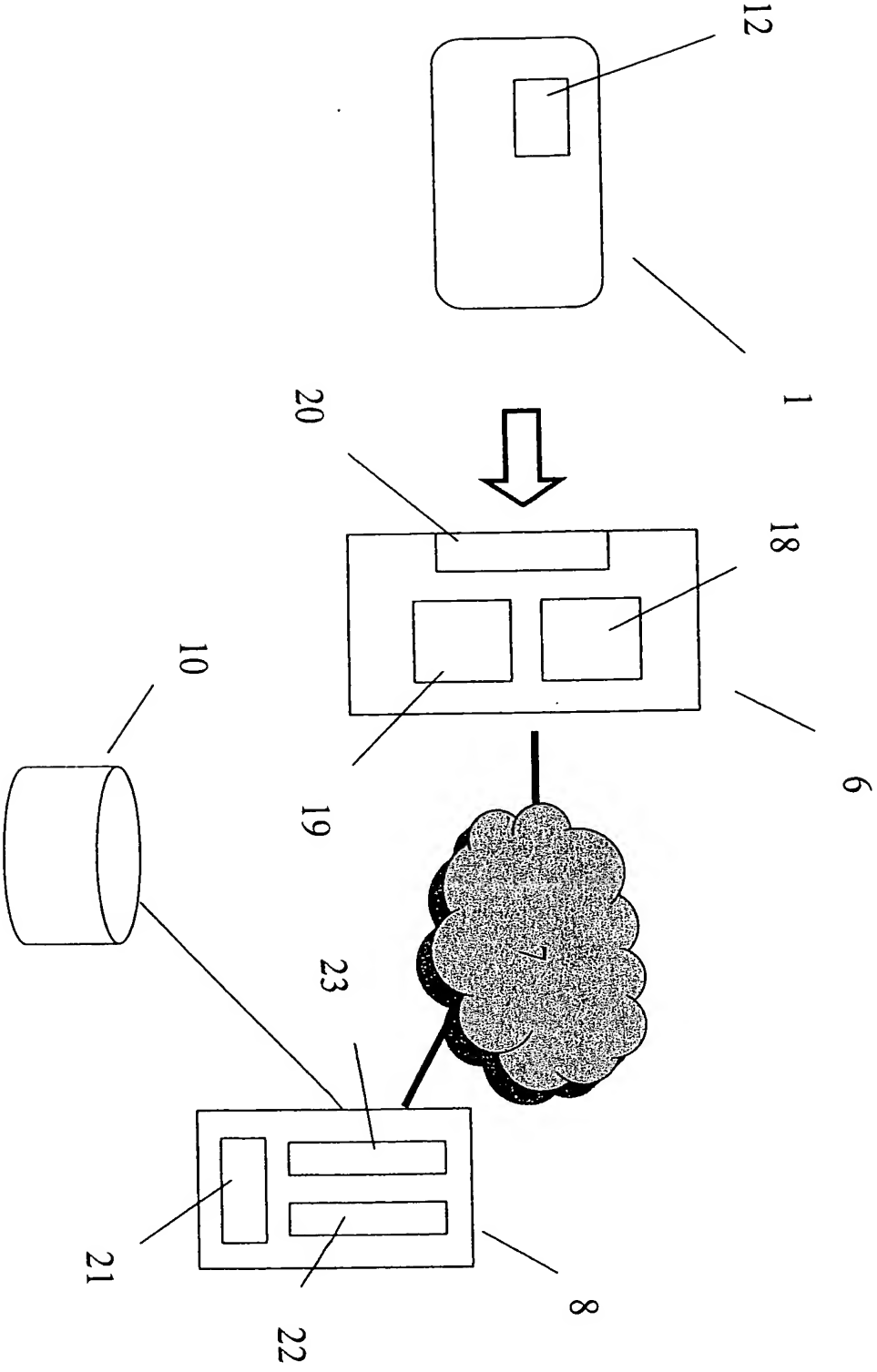
18. A terminal (6) that is connected to an infrastructure comprising a network (7) and a server (8) of a service provider, whereby the terminal is equipped with a terminal processor (18) and terminal input/output devices (20) to be able to communicate with an electromagnetic scratchcard according to one of the foregoing claims, such terminal processor (18) being arranged to send the electronic data received from the electromagnetic scratchcard (1) over the network (7) to the server (8), and to send the electronic or magnetic data received from the server (8) to the electromagnetic scratchcard (1) and to read out a challenge (5) present on the electromagnetic scratchcard (1) to determine the status of the electromagnetic scratchcard (1).

19. A server (8) that is connected to an infrastructure not directly accessible to a service customer, such infrastructure comprising a network (7) of a service provider, and connected to a database (10), such server (8) being arranged to:
- receive from a terminal (6) electronic or magnetic data via the network (7);
- compare the electronic or magnetic data received from the terminal (6) with the electronic or magnetic data contained in the database (10);
- retrieve electronic or magnetic data from the database (10) on the basis of electronic or magnetic data received from the terminal (6) and send such data via the network (7) to the terminal (6);

- modify electronic or magnetic data in the database (10) based on electronic or magnetic data received from the terminal (6);
- retrieve from the database (10) an activation challenge (9) associated with a card ID (2) and send it via the network (7) to the terminal (6), such card ID (2) received via the terminal uniquely defining an electromagnetic scratchcard.

20. A server (8) according to claim 19, whereby the server (8) is arranged to reduce de card balance (13) in the database (10) depending upon a service provided to the user of the electromagnetic scratchcard.

FIG. 1



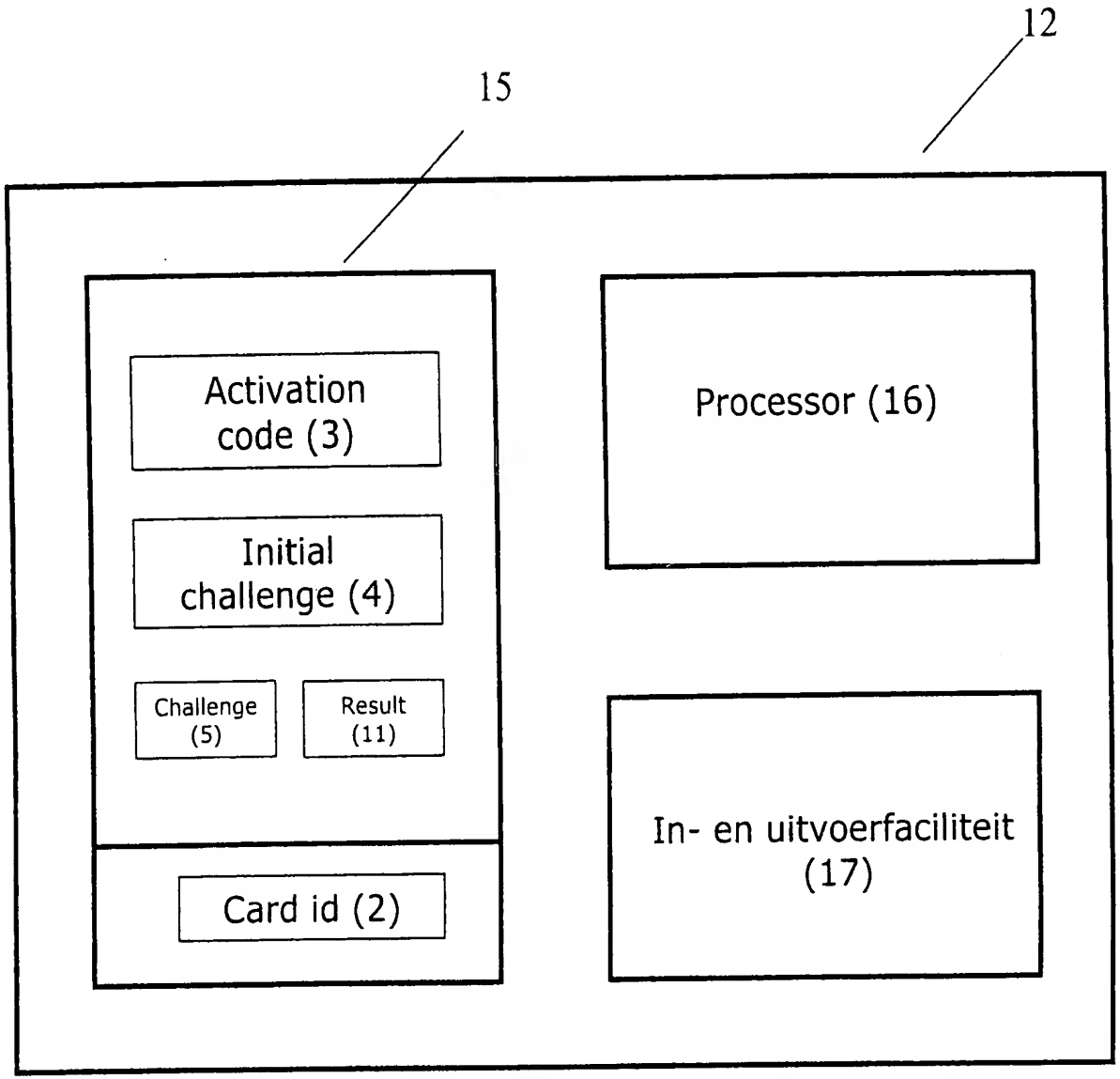


FIG. 2

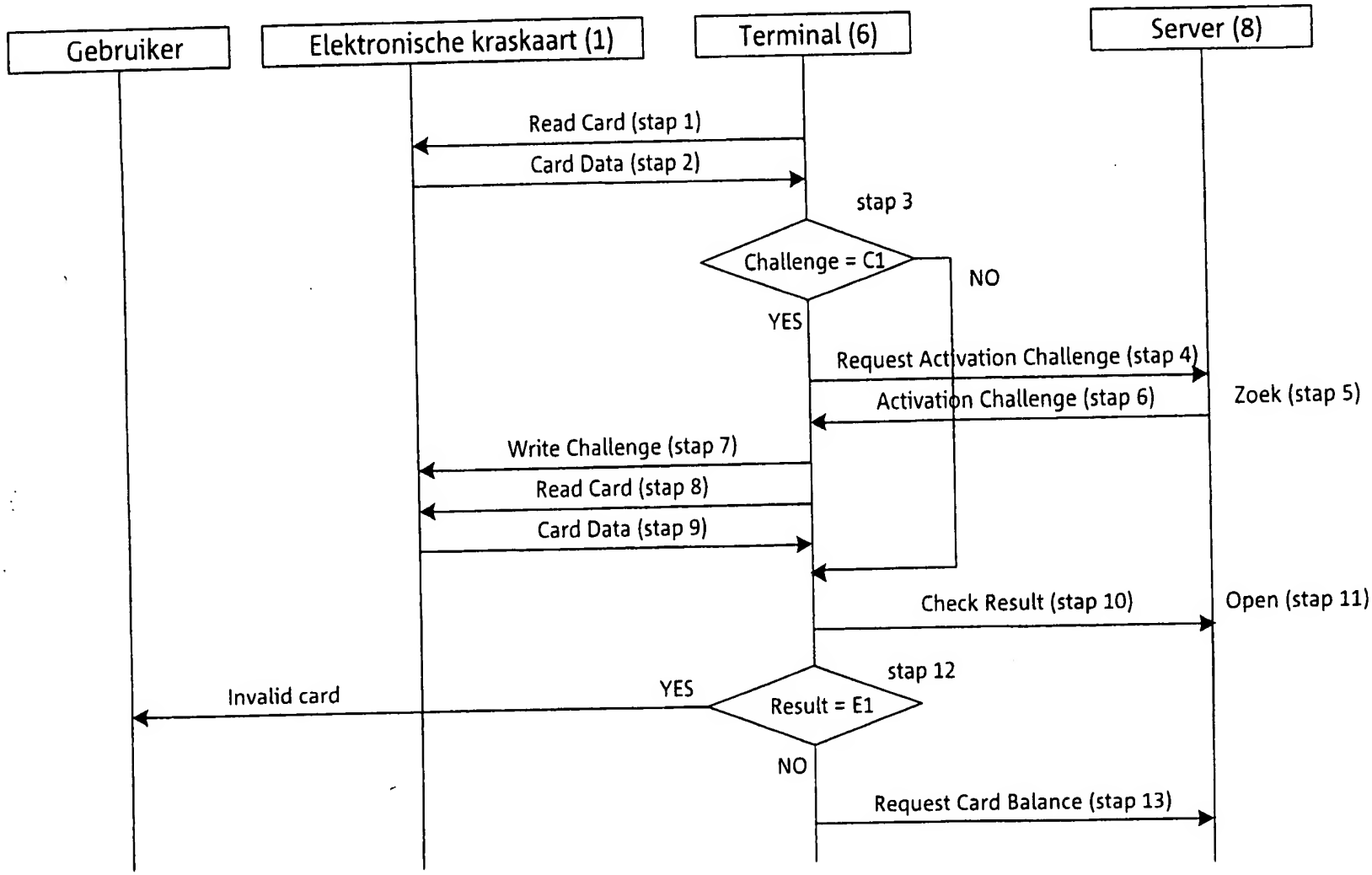


FIG. 3

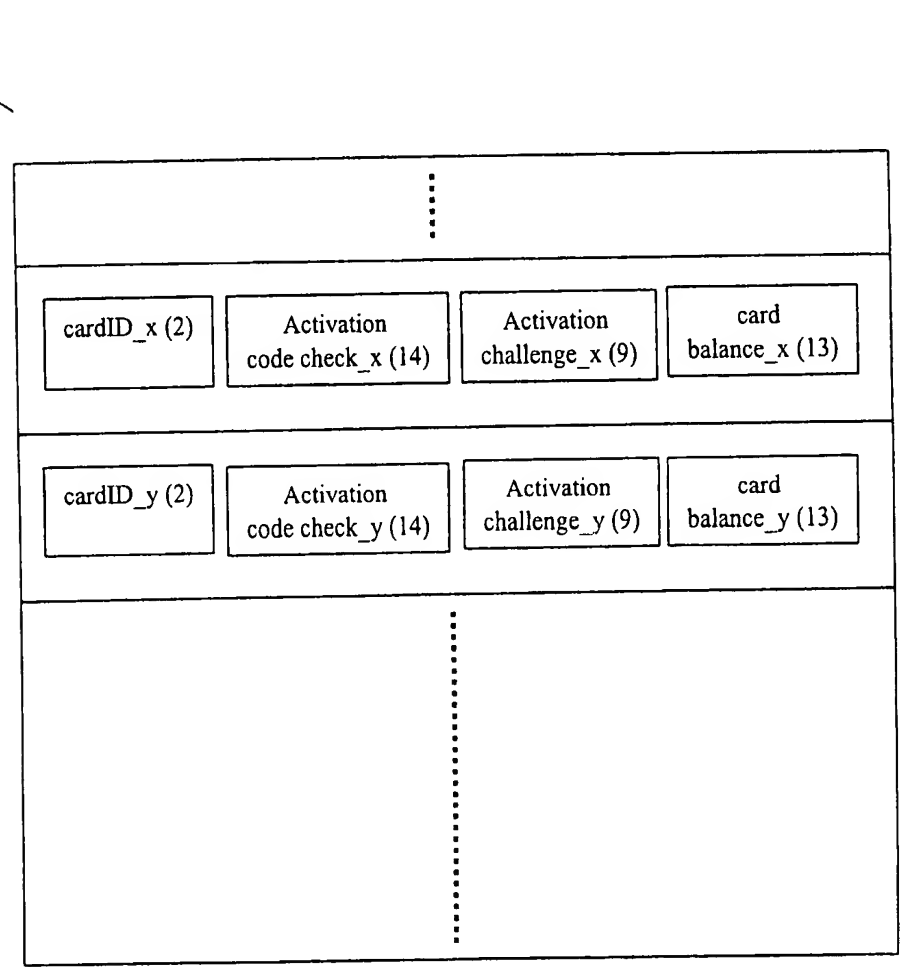


FIG. 4